WHAT IS CLAIMED IS:

1. A method of decoding an error-correction code in a data signal, comprising the steps of:

receiving the data signal at a decoding unit;

computing a plurality of syndromes associated with the data signal using the decoding unit;

generating an error polynomial from the data signal using one or more Galois field multiply accumulators each of which contains a Galois field multiplier feeding a Galois field adder; and

locating errors within the data signal using the error polynomial.

2. The method of Claim 1 wherein the Galois field multiplier operates in a multiply pass-through mode by selecting a "1" value as an operand input.

3. The method of Claim 1 wherein the Galois field adder operates in an addition pass-through mode by selecting a "0" value as an operand input.

4. The method of Claim 1 further comprising the steps of:

detecting a zero operand of the Galois field multiply accumulator; and

setting a zero operand latch in response to said detecting step.

5. The method of Claim 1 wherein said computing, extracting, and locating steps use a Bose-Chaudhuri-Hocquenghem (BCH) code.

6. The method of Claim 1 wherein said computing steps computes 2t syndromes, where t is a number of correctable errors which the error-correcting code can correct.

7. The method of Claim 1 wherein said computing step uses a linear feedback register to compute the syndromes.

8. The method of Claim 1 wherein said computing step includes the steps of:
dividing a received code word in the data signal by a minimal Galois polynomial; and
evaluating a remainder from said dividing step.

9. The method of Claim 1 wherein said generating step generates the error polynomial based on no more than six equations having no more than two branch decisions.

10. The method of Claim 1 wherein said generating step includes the step of the Galois field multiply accumulator performing a Galois field multiply/accumulate operation in a single clock cycle.

11. The method of Claim 1 wherein said generating step includes the step of calculating correction terms using the Galois field multiply accumulators based on the syndromes.

12. The method of Claim 1 wherein said locating step locates the errors by determining roots of the error polynomial which correspond to error locations.

13. The method of Claim 11 wherein said locating step uses Chien's algorithm to search for the error location numbers.

14. A method of determining an error polynomial for decoding a Bose-Chaudhuri-Hocquenghem (BCH) code, comprising the steps of:
computing a plurality of syndromes associated with a data signal having a BCH code embedded therein;
feeding the syndromes to a plurality of Galois field multiply accumulators;
calculating a plurality of minimum-degree polynomials associated with the BCH code, using the Galois field multiply accumulators; and
generating an error polynomial based on the minimum-degree polynomials.

15. The method of Claim 14 wherein said calculating step includes the step of calculating a plurality of coefficients of at least one of the minimum-degree polynomials.

16. The method of Claim 14 wherein each of the plurality of Galois field multiply accumulators represents a different power of the error polynomial.

17. The method of Claim 14 wherein said calculating step includes the step of computing a first correction term using at least one of the Galois field multiply accumulators, the first correction term being equal to a first one of the syndromes.

18. The method of Claim 17 wherein said calculating step includes the step of computing a second correction term using at least one of the Galois field multiply accumulators, the second correction term being equal to the sum of a product of the first syndrome with a second one of the syndromes, and a third one of the syndromes.

19. The method of Claim 17 wherein said step of computing the first correction term includes the step of operating the at least one Galois field multiply accumulator in a pass-through mode.

20. The method of Claim 14 wherein:
the BCH code is a triple-error correcting code; and
said calculating step calculates at least three minimum-degree polynomials.

21. The method of Claim 20 wherein said calculating step further includes the steps of:
computing a first correction term using at least one of the Galois field multiply accumulators, the first correction term being equal to a first one of the syndromes;
computing a second correction term using at least one of the Galois field multiply accumulators, the second correction term being equal to the sum of a product of the first syndrome with a second one of the syndromes, and a third one of the syndromes; and

computing a third correction term using at least one of the Galois field multiply accumulators, the third correction term being based in part on coefficients of at least one of the minimum-degree polynomials.

22. The method of Claim 21 wherein said calculating step includes the step of determining whether the second correction term is equal to zero.

23. The method of Claim 22 wherein said calculating step equates a first one of the minimum-degree polynomials to a second one of the minimum-degree polynomials in response to a determination that the second correction term is equal to zero.

24. The method of Claim 21 wherein said calculating step includes the step of determining whether the third correction term is equal to zero.

25. The method of Claim 24 wherein said calculating step equates a first one of the minimum-degree polynomials to a second one of the minimum-degree polynomials in response to a determination that the third correction term is equal to zero.

26. The method of Claim 20 wherein there are exactly four of the Galois field multiply accumulators, and said calculating step includes the step of controlling inputs to the Galois field multiply accumulators using a state machine.

27. The method of Claim 26 wherein the Galois field multiply accumulators perform a Galois field multiply/accumulate operation in a single clock cycle.

28. A Galois field multiply accumulator comprising:

a Galois field multiplier having two operand inputs and an output;

a Galois field adder having two operand inputs and an output, said output of said Galois field multiplier being connected to a first one of said inputs of said Galois field adder;

a first multiplexer having at least two inputs, a select line, and an output, said output of said first multiplexer being coupled to a first one of said

inputs of said Galois field multiplier, a first one of said inputs of said first multiplexer being connected to a first data line, and a second one of said inputs of said first multiplexer being connected to a constant zero value;

a second multiplexer having at least two inputs, a select line, and an output, said output of said second multiplexer being coupled to a second one of said inputs of said Galois field multiplier, a first one of said inputs of said second multiplexer being connected to a second data line, and a second one of said inputs of said second multiplexer being connected to a constant one value; and

a third multiplexer having at least two inputs, a select line, and an output, said output of said third multiplexer being coupled to a second one of said inputs of said Galois field adder, a first one of said inputs of said third multiplexer being connected to a third data line, and a second one of said inputs of said third multiplexer being connected to a constant zero value.

29. The Galois field multiply accumulator of Claim 28 wherein said output of said Galois field adder is connected to a third one of said inputs of said first multiplexer.

30. The Galois field multiply accumulator of Claim 29 wherein said output of said Galois field adder is connected to a third one of said inputs of said third multiplexer.

31. The Galois field multiply accumulator of Claim 28 wherein said output of said Galois field adder is connected to a third one of said inputs of said third multiplexer.

32. The Galois field multiply accumulator of Claim 28 further comprising means for detecting a zero output of said Galois field adder.

33. The Galois field multiply accumulator of Claim 28 further comprising control means for activating said select line of said first multiplexer to enable a pass-through mode.

34. The Galois field multiply accumulator of Claim 33 wherein said control means further activates said select line of said third multiplexer to enable the pass-through mode.

35. The Galois field multiply accumulator of Claim 28 wherein said Galois field multiplier, said Galois field adder, and said first, second and third multiplexers are formed in a common application-specific integrated circuit.

36. A decoder circuit comprising:
a plurality of syndrome inputs;
a plurality of Galois field multiply accumulators; and
means for using said Galois field multiply accumulators to generate an error polynomial based on values provided at said syndrome inputs.

37. The decoder circuit of Claim 36 wherein each of said plurality of Galois field multiply accumulators represents a different power of the error polynomial.

38. The decoder circuit of Claim 36 wherein said using means uses said Galois field multiply accumulators to generate an error polynomial for a Bose-Chaudhuri-Hocquenghem (BCH) triple-error correcting code.

39. The decoder circuit of Claim 36 wherein said using means includes a state machine which asserts control ports on said Galois field multiply accumulators to generate the error polynomial.

40. The decoder circuit of Claim 36 wherein said Galois field multiply accumulators perform a Galois field multiply/accumulate operation in a single clock cycle.

41. The decoder circuit of Claim 36 wherein said using means uses the Galois field multiply accumulators to calculate a plurality of minimum-degree polynomials associated with a Bose-Chaudhuri-Hocquenghem (BCH) code.

42. The decoder circuit of Claim 41 wherein said using means uses the Galois field multiply accumulators to calculate a plurality of coefficients of at least one of the minimum-degree polynomials.

43. The decoder circuit of Claim 41 wherein said using means extracts an error-generation polynomial from the syndromes based on no more than six equations having no more than two branch decisions executed by said Galois field multiply accumulators.

44. The decoder circuit of Claim 36 wherein said using means includes means for operating a selected one or more of said Galois field multiply accumulators in a pass-through mode.

45. The decoder circuit of Claim 36 wherein at least one of said Galois field multiply accumulators comprises:

a Galois field multiplier having two operand inputs and an output;

a Galois field adder having two operand inputs and an output, said output of said Galois field multiplier being connected to a first one of said inputs of said Galois field adder;

a first multiplexer having at least two inputs, a select line, and an output, said output of said first multiplexer being coupled to a first one of said inputs of said Galois field multiplier, a first one of said inputs of said first multiplexer being connected to a first data line, and a second one of said inputs of said first multiplexer being connected to a constant zero value;

a second multiplexer having at least two inputs, a select line, and an output, said output of said second multiplexer being coupled to a second one of said inputs of said Galois field multiplier, a first one of said inputs

of said second multiplexer being connected to a second data line, and a second one of said inputs of said second multiplexer being connected to a constant one value; and

a third multiplexer having at least two inputs, a select line, and an output, said output of said third multiplexer being coupled to a second one of said inputs of said Galois field adder, a first one of said inputs of said third multiplexer being connected to a third data line, and a second one of said inputs of said third multiplexer being connected to a constant zero value.

46. An OC-192 input/output card comprising:

four OC-48 processors; and

an OC-192 front-end application-specific integrated circuit (ASIC) connected to said four OC-48 processors, said OC-192 front-end ASIC having means for de-interleaving an OC-192 signal to create four OC-48 signals, and means for decoding error-correction codes embedded in each of the four OC-48 signals, said decoding means including a plurality of Galois field multiply accumulators.

47. The OC-192 input/output card of Claim 46 wherein said Galois field multiply accumulators perform a Galois field multiply/accumulate operation in a single clock cycle.

48. The OC-192 input/output card of Claim 46 wherein said decoding means uses said Galois field multiply accumulators to generate an error polynomial for a Bose-Chaudhuri-Hocquenghem (BCH) triple-error correcting code.

49. The OC-192 input/output card of Claim 48 wherein each of said plurality of Galois field multiply accumulators represents a different power of the error polynomial.

50. The OC-192 input/output card of Claim 48 wherein said decoding means includes means for dividing a received code word in a given one of the OC-48 signals by a minimal Galois polynomial, and evaluating a remainder from said dividing step

51. The OC-192 input/output card of Claim 48 wherein said decoding means locates errors by determining roots of the error polynomial which correspond to error locations.

52. The OC-192 input/output card of Claim 48 wherein said decoding means operates at least one of the Galois field multiply accumulators in a pass-through mode.

53. The OC-192 input/output card of Claim 48 wherein said decoding means calculates a plurality of minimum-degree polynomials associated with the BCH code, using the Galois field multiply accumulators.

54. The OC-192 input/output card of Claim 48 wherein said decoding means includes a state machine which asserts control ports on said Galois field multiply accumulators to generate the error polynomial.